Computer Incident, Intrusion, Emergency Response Audit Program
Created by Deborah Coggins
May 2001

Audit Objectives:

- To ensure assets are adequately monitored and protected.
- To ensure the computer incident, intrusion detection, or emergency response process policies and procedures are consistent with industry standards and good business practices.
- To ensure tools necessary to prevent or detect an attempted computer incident or intrusion have been purchased and appropriate users have been adequately trained.
- To ensure roles and responsibilities of key positions necessary to respond to a computer incident, intrusion, or emergency have been developed and communicated.
- To ensure computer incidents, intrusion attempts, and emergencies are escalated to appropriate management levels consistent with industry standards and good business practices.

Audit Scope:

- Review and evaluate all policies, procedures, and forms developed for the computer incident, intrusion, or emergency response process.
- Review and evaluate the risk assessment process uses to determine the computer incident, intrusion, or emergency response process.
- Review and evaluate the purchase of tools designed to prevent and detect a computer incident or intrusion.
- Review and evaluate user training on the computer incident or intrusion detection tools.
- Review and evaluate the roles and responsibilities of key positions that have been identified as necessary to respond to computer incident, intrusion, or emergency.
- Review and evaluate the computer incident, intrusion, or emergency escalation process.

Control Objective	Expected Results
A. Review and evaluate all computer incident, intrusion detection, or emergency response process policies, procedures, and forms to ensure they are consistent with industry standards and good business practices.	
Audit Step 1. Obtain a copy of all polices and procedures used to the address computer incidents, intrusions, or emergency responses process.	A current copy of all policies and procedures should be available. NOTE: It will be difficult to continue the audit of the computer incident, intrusion, and emergency response processes if policies, procedures and forms have not been developed. However, the information technology auditor should continue and make recommendation based on industry standards and good business practices.

Control Objective	Expected Results
Audit Step 2. Review and determine if the policies and procedures are consistent with industry standards and good business practices.	At a minimum the following topics should be included: --Mission statement --Security policies --Risk assessment --Information classification --Recovery process --Prosecution --Handling publicity --Regular monitoring CERT advisories --Glossary (e.g., incident, event, types of incidents) --Contacting law enforcement --How incidents or emergencies are detected and resolved --Maintaining evidence --Establishing secure communications --Contact information (names, telephone numbers, fax numbers) for response team --User training --Handling information that results from an incident, intrusion or emergency
Audit Step 3. Review and evaluate how updates (additions, modification, and deletions) to the policies and procedures are performed.	A process to determine who, when, and how updates to the policies and procedures are performed should exist. Management must have the assurance current, accurate information is maintained.
Audit Step 4. Select a sample of updated policies and procedures. Determine if the selected policies and procedures have followed the procedures defined in Audit Step 3.	The sample should follow the process provided in Audit Step 3 for updating policies and procedures.
Audit Step 5. Determine if a periodic review of policies and procedures is performed.	A process to periodically review (i.e., quarterly or semi-annually) policies and procedures helps management ensure updates have not been overlooked.

Control Objective	Expected Results
Audit Step 6. Select a sample of policies and procedures to ensure they have undergone the periodic review process. Determine if the process described in Audit Step 5 is being followed.	The sample should follow the process provided in Audit Step 5 for the periodic review of policies and procedures.
Audit Step 7. Review and evaluate how the policies and procedures are distributed to the appropriate individuals.	Developing a process for the distribution of policies and procedures helps management ensure employees possess current, accurate information.
Audit Step 8. Select a sample of policies and procedures. Determine if they have been distributed to the appropriate individuals.	The sample should follow the process provided in Audit Step 7 for the distribution policies and procedures.
B. Review and evaluate the risk assessment process to ensure assets (i.e., hardware, software, and information) are appropriately protected, consistent with industry standards and good business practices.	
Audit Step 9. Review and evaluate how the initial risk assessment process was performed.	At a minimum the following topics should have been addressed: --Assets (what needs to be protected/monitored); --Threats (who would be interested in the assets) --Vulnerabilities (what technical holes could and do exist) --Consequences (what is the worst case scenario(s) if a computer incident, intrusion or emergency occurs) --Likelihood of a threat (what have been other business' or organization's experiences).
Audit Step 10. Review and evaluate how the risk assessment process is performed for new projects/processes/systems.	Developing a risk assessment process identical to the initial risk assessment to be performed for new projects/processes helps management ensure new projects/processes are adequately protected by the computer incident, intrusion, and emergency response process.
Audit Step 11. Select a sample of new projects/processes/systems. Determine if the sample has undergone the risk assessment described in Audit Step 10.	The sample should follow the process provided in Audit Step 10 for the risk assessment of new projects/processes.

Control Objective	Expected Results
Audit Step 12. Review and evaluate the process to periodically reassess the current environment.	A process should exist to periodically reassess the current environment. The process should include the initial assumptions, any changes to the environment or project/process since the initial assessment, and any future plans for the project/process. Developing a periodic reassessment helps management ensure the risks previously identified are still valid, changes to the environment have been taken into consideration, and plans for future changes have been considered.
Audit Step 13. Review the last reassessment of the current environment. Determine if the process described in Audit Step 12 has been followed.	The last reassessment should follow the process provided in Audit Step 12
C. Review and determine if the tools that have been purchased to prevent and/or detect a computer incident or intrusion are consistent with industry standards and good business practices.	
Audit Step 14. Obtain a complete inventory of the tools that have been purchased to prevent and/or detect a computer incident or intrusion.	A current inventory of the tools should be available. The inventory should include name of the tool, manufacturer, date of purchase/ acquisition, date of renewal of maintenance contract (if required) and date tool was replace or not longer available for use.
Audit Step 15. Select a sample inventory of tools. Interview the tools users and determine if the process described in Audit Step 14 is being followed.	The sample should determine if the tools listed are still current or if they have been replaced.

Control Objective	Expected Results
Audit Step 16. Determine and evaluate activities the tools detect and/or monitor.	At a minimum the tools should address the following: --Network Monitoring (tools such as Argus or Swatch) --Authentication/Password (tools such as CRACK or OPIE) --Service-Filtering (tools such as TCP/IP wrapper) --Scanning Hosts for known Vulnerabilities (tools such as ISS or SATAN) --Multi-purpose (tools such as COPS) --Integrity-Checking (tools such as MD5 or Tripware) --Sendmail (tools such as smrsh) --Report writer (tools such as SARA) --Firewall, Proxy, and Filtering (tools such as fwtk, ipfirewall, or SOCKS) --Secure Remote Access/Authorization (tools such as RADIUS, SSL, SSH, or Kerberos)
Audit Step 17. Determine and evaluate the process to ensure the most current release or version of the tools is in use.	The process should include procedures to obtain the following: --updates --patches
Audit Step 18. Determine and evaluate the process for evaluating new tools as they are made available for use.	The process would ensure the latest and greatest tools are evaluated and purchased as they become available.
D: Review user training on tools designed to prevent and detect a computer incident or intrusion.	
Audit Step 19. Obtain a list of employees who use the tools.	A current list of employees who use the tools should be available.
Audit Step 20. Obtain the employee training schedule for the employees who are to use the tools.	A training schedule ensures the employees listed in Audit Step 19 have undergone the proper training.
Audit Step 21. Determine the process for reassignment of tools usage to employees as a result of promotions, resignations, or retirement. The process should include a training schedule.	A process should exist to assign tool usage to other employees as required as a result of promotions, resignations, or retirement.

Control Objective	Expected Results
E: Review the roles and responsibilities of key positions that have been identified as necessary to respond to computer incident, intrusion, or emergency.	
Audit Step 22. Obtain an organization chart that identifies positions/employees who are responsible for the computer incident, intrusion, or emergency process.	The following positions should be included: --Security Office Representative --Network Services Representative --Platform Representatives (e.g., UNIX, Windows NT, Novell, and Windows 2000) --Fraud specialist --Legal counsel --Information Technology Auditor
Audit Step 23. Evaluate the positions/employees that appear on the organization chart obtained in Audit Step 22.	The positions/employees ensures at a minimum the following: --The reporting structure supports the process. --The position the employee holds matches the needs of the computer incident, intrusion, or emergency process. --No obvious positions are missing. --All positions have been filled or are in the process of being filled. (Positions should not be vacant for an extended period of time.)
Audit Step 24. Interview a sample of employees that appear on the list obtained in Audit Step 22 to determine if they have a clear understanding of their role and responsibilities. This should include their experiences during the most recent computer incident, intrusion, or emergency.	Employees have a clear understanding of their role and responsibility.

Control Objective	Expected Results
F. Review the computer incident, intrusion, or emergency escalation process.	
Audit Step 25. Obtain a copy of the computer incident, intrusion, or emergency escalation process.	The process should include: --verify an incident, intrusion or emergency has actual occurred --secure internal lines of communication --notification of appropriate employees --elimination of the cause of the problem --recovery of the affected systems --when law enforcement should be involved --determine if the public will be notified --how the process will be updated and distributed to the appropriate employees
Audit Step 26. Select a sample of actual incident, intrusion or emergencies to determine if escalation process was followed as described in Audit Step 25.	The sample should determine if the process described in Audit Step 25 has been followed.

Sources of information

"Audit Evidence Requirement." IS Auditing Guideline. Information Systems Audit and Control Association.

"Audit Sampling." IS Auditing Guideline. Information Systems Audit and Control Association.

"COBIT Audit Guidelines." COBIT. 3rd ed. Information Systems Audit and Control Foundation.

"COBIT Control Objectives." COBIT. 3rd ed. Information Systems Audit and Control Foundation.

"COBIT Management Guidelines." COBIT. 3rd ed. Information Systems Audit and Control Foundation.

"Computer Security Incident Handling: Step-by-Step." System Administration Networking and Security (SANS) Institute Publications.

"Computer Security Incident Response Policy." The Center for Information Technology.

"Detecting Signs of Intrusion." CERT Coordination Center. Carnegie Mellon Software Engineering Institute.

"Establish policies and procedures for responding to intrusions." CERT Coordination Center.

"Expectations for Computer Security Incident Response." The Internet Society.

"Incident Reporting Guidelines." CERT Coordination Center.

Responding to Intrusions by Klaus-Peter Kossakowski

"List of Security Tools." CERT Coordination Center.

Network Intrusion Detection An Analyst's Handbook by Stephen Northcutt

"Planning The IS Audit." IS Auditing Guideline. Information Systems Audit and Control Association.

"Prepare to respond to intrusions." CERT Coordination Center.
"Responding to Intrusions." CERT Coordination Center.
Forming an Incident Response Team by Danny Smith
"Standards for Information Systems Auditing." IS Auditing Guideline. Information Systems Audit and Control Association.
NSA Glossary of Terms Used in Security and Intrusion Detection by Greg Stocksdale
How to Form a Skilled Computer Incident Response Team by Peter Stephenson
"Use of Risk Assessment in Audit Planning." IS Auditing Guideline. Information Systems Audit and Control Association.
Handbook for Computer Security Incident Response Teams (CSIRTs) by Moira J. West-Brown, Don Stikvoort, and Klaus-Peter Kossakowski.